UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/506,943	03/07/2005	Carl Gustavsson	9562-9	8802

20792 7590 07/27/2009

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
PHAM, LUU T	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
07/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/506,943	GUSTAVSSON ET AL.	
	Examiner	Art Unit	
	LUU PHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *46-51 and 53-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *46-51 and 53-57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Amendment filed on 04/28/2009.

2. In the instant Amendment, Claims 1-45, 52, and 58-75 were cancelled; Claim 46 has been amended; and Claim 46 is independent claim. Claims 46-51 and 53-57 have been examined and are pending. **This Action is made FINAL.**

Response to Arguments

3. The objections to the claims 46, 59, and 69 under 35 U.S.C. 132(a) are withdrawn as the claims have been amended/canceled.

4. The rejections of claims 59-75 under 35 U.S.C. § 101 are withdrawn as the claims have been canceled.

5. The rejections of claims 59-75 under 35 U.S.C. § 112 second paragraph are withdrawn as the claims have been canceled.

6. Applicants' arguments with respect to claim 46 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. **Claims 46-49 and 54-57 are rejected under 35 U.S.C. 103(a)** as being unpatentable over *"SyncML Sync Protocol, version 1.0,"* (hereinafter "SyncML"), *SYNCML CONSORTIUM*, published on December 07, 2000, in view of *"SyncML Device Management Security, Version 1.1"* (hereinafter "SyncML-DMS"), *SYNCML CONSORTIUM*, published on February 15, 2002, in view of Quick, Jr. et al., (hereinafter "Quick"), U.S. Patent Application No. 2002/0091933, filed on May 22, 2001, in view of Beatson, U.S. Patent Application No. 2003/0056100, filed on September 14, 2001, and further in view of Lahteenmaki, U.S. Patent Application No. 2003/0028805, filed on August 03, 2001.

- **Regarding claim 46**, SyncML discloses a method for providing authentication when messages are sent between an electronic communication apparatus and a server according to a synchronization protocol *(page 8, Fig. 2; page 20, section 3: authentication)* in which a plurality of different authentication methods are available *(pages 20-27; auth-*

basic and auth-MD5 are known as plurality of different authentication methods), comprising:

providing an authentication method indicator *(pages 20-27, sections 3.5 and 4.1; XML Tag 'type'; see also page 13, section 2.5)* that specifies an authentication method of the plurality of different authentication methods *(pages 20-27; auth-basic and auth-MD5 are known as plurality of different authentication methods)* according to which the authentication is to be executed *(page 20, section 3; page 21, section 3.5; XML Tag 'SyncML' and 'VerDTD')*;

incorporating into a message the authentication method indicator *(pages 20-27; section 3.5.1; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-basic>; section 3.5.2; Pkg #1 (with credentials) from client; XML Tag 'type' <auth-md5>; section 4.1.1; page 13, section 2.5; both the sync client and server can challenge for the authentication and the device receiving the authentication challenge must be able to send the authorization credentials back; see also pages 26-30 and 34-40)* comprising a plurality of authentication capabilities of the communication apparatus *(page 13, section 2.5; the protocol requires the support for the basic authentication and the MD5 digest access authentication; pages 21-27, section 3.5.1; XML Tag 'type' <auth-basic>; XML Tag 'type' <auth-md5>; see also pages 26-30 and 34-40)* among the plurality of different authentication methods *(pages 20-27; auth-basic and auth-MD5 are known as plurality of different authentication methods)*; and

transmitting said message to said server according to an authentication protocol of the synchronization protocol *(page 22; Pkg #1 (with credentials) from client; data inside*

XML Tag 'type'<auth-basic>; page 23; Pkg #1 (with credentials from Client; syncML: <auth-md5>; see also page 27; section 4.1.1: 'Example of Sync Initialization of Packet from Client').

SyncML does not explicitly disclose generating, at the server, an authentication data value comprising an equivalent of an AKA FRESH parameter; and sending the authentication data value to the electronic communication apparatus;

However, in an analogous art, SyncML-DMS discloses a SyncML Device Management protocol, comprising steps of generating, at the server, an authentication data value comprising an equivalent of an AKA FRESH parameter *(SyncML-DMS: page 6, section 4: Credentials; a none is used to allow for prevention of replay attacks; see also page 11)*; and

sending [[the integrity key and]] the authentication data value to the electronic communication apparatus *(SyncML-DMS: page 6; section 4: Credentials; for the purpose of Server to Device authentication, a Server ID, password and nonce are required; see also pages 7-11; sections 6-7)*;

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of SyncML-DMS with the method of SyncML to include steps of generating, at the server, an authentication data value comprising an equivalent of and AKA FRESH parameter; and sending the authentication data value to the electronic communication apparatus to provide users with a means for preventing of replay attacks using authentication data *(SyncML-DMS: page 6)*.

SyncML and SyncML-DMS do not explicitly disclose generating, at the server, an integrity key; sending the integrity key to the electronic communication apparatus; using the integrity key at the electronic communication apparatus to generate MAC values; and using a hashing function at the electronic communication apparatus to compute a Hashed Method Authentication Code (HMAC) on the message.

However, in an analogous art, Quick discloses a method for providing local authentication, wherein generating, at the server, an integrity key *(Quick: par. 0024; key generator 250 generates a cryptographic cipher key (CK) 290 and an integrity key (IK) 310)*;

sending the integrity key to the electronic communication apparatus *(Quick: pars. 0024 and 0026-0027; IK 310 is conveyed to the mobile unit 220)*;

using the integrity key at the electronic communication apparatus to generate MAC values *(Quick: pars. 0026; the IK 310 can be used to generate a message authentication code MAC)*; and

using a hashing function at the electronic communication apparatus to compute a Hashed Method Authentication Code (HMAC) on the message *(Quick: par. 0038; HMAC-SHA-1 scheme; HMAC is implemented in the subscriber identification token).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Quick with that of SyncML to including steps of generating, at the server, an integrity key; sending the integrity key to the electronic communication apparatus; using the integrity key at the electronic communication apparatus to generate MAC values; and using a hashing function

at the electronic communication apparatus to compute a Hashed Method Authentication Code (HMAC) on the message to provide users with a mean for providing secure authentication to a subscriber roaming outside his or her home system *(Quick: par. 0007)*.

SyncML, SyncML-DMS and Quick disclose all limitations as recited above, but do not explicitly disclose the integrity key is encrypted with the public key of the electronic communication apparatus.

However, in an analogous art, Beatson discloses a method for authenticating a digitized signature for execution of an electronic document, wherein the integrity key is encrypted with the public key of the electronic communication apparatus *(Beatson: par. 0080; the device (server) encrypts the secret key (integrity key) with the public key of the destination host (electronic communication apparatus) and communicates the data to that host with the encrypted secret key)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Beatson with that of SyncML, SyncML-DMS and Quick, wherein the integrity key is encrypted with the public key of the electronic communication apparatus to provide users with a means for providing authenticating access to an electronic system *(Beatson: par. 0003)*.

SyncML, SyncML-DMS Quick, and Beatson disclose all limitations as recited above, but do not explicitly disclose the specified authentication method is any of a group comprising Wireless Public Key Identity (WPKI), Wireless Identity Module (WIM) authentication.

However, in an analogous art, Lahteenmaki discloses a method for managing network service access and enrolment, wherein the authentication method is WPKI or WIM authentication *(Lahteenmaki: pars. 0038 and 0055; WAP Public key Infrastructure (WPKI) provides a manner of enabling the trust relationships needed for authentication of servers and clients; WIM card manufacturer certificate).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Lahteenmaki with that of SyncML wherein the authentication method is WPKI or WIM authentication to provide users with a means for managing user access and enrollment for secure network services *(Lahteenmaki: par. 0001).*

- **Regarding claim 47**, SyncML, SyncML-DMS, Quick, Beatson, and Lahteenmaki disclose the method according to claim 46.

SyncML further discloses the authentication method indicator is incorporated into a meta command of the synchronization protocol *(SyncML: page 22, Pkg #1 (with credentials) from Client; XML Tag 'Meta' includes <auth-basic>; page 23; Pkg #1 (with credentials) from Client; see also page 27; section 4.1.1: 'Example of Sync Initialization of Packet from Client').*

- **Regarding claim 48**, SyncML, SyncML-DMS, Quick, Beatson, and Lahteenmaki disclose the method according to claim 46.

SyncML further discloses the message is an initialization message *(SyncML: pages 22-25; Pkg #1 (with credentials) from Client; Fig. 6; Pkg #1: client initialization*

package to server), and the authentication capabilities of the electronic communication apparatus is indicated in an authentication method list of the initialization message *(SyncML: page 15, section 2.7; pages 22-24, section 3.5; pages 25-27, section 4)*, which is sent to the server for establishing a connection *(SyncML: page 25; Fig. 6; Pkg #1: client initialization package to server)*.

- **Regarding claim 49**, SyncML, SyncML-DMS, Quick, Beatson, and Lahteenmaki disclose the method according to claim 46.

SyncML further discloses any authentication data relating to the specified authentication method is incorporated in a data string of the message-sent according to the synchronization protocol *(SyncML: page 21, section 3.5; the client sends Pkg #1 with the credentials; the server accepts the credentials and the session is authenticated; see also page 25; Fig. 6)*.

- **Regarding claim 50**, SyncML, SyncML-DMS, Quick, Beatson, and Lahteenmaki disclose the method according to claim 46.

Quick further discloses the authentication method is Global System for Mobile communication (GSM) Subscriber Identify Module (SIM) authentication *(Quick: pars. 0005-0006; Subscriber Identity Module (SIM) is used in GSM system; an authentication key for identifying the subscriber)*.

- **Regarding claim 51**, SyncML, SyncML-DMS, Quick, Beatson, and Lahteenmaki disclose the method according to claim 46.

Quick further discloses the authentication method is Universal Mobile Telephone System (UMTS) Universal Subscriber Identity Module (USIM) authentication, which provides server authentication *(Quick: pars. 0005 and 0006; next generation SIM card have been renamed as USIM used in UTMS system; an authentication key for identifying the subscriber)*.

- **Regarding claim 54**, SyncML, SyncML-DMS, Quick, Beatson, and Lahteenmaki disclose the method according to claim 48.

SyncML further discloses determining at the server the authentication capabilities of the electronic communication apparatus based on the plurality of authentication capabilities listed in the authentication method list *(SyncML: page 20, section 3.1-3.3; page 21, section 3.5.1; the client sends Pkg #1 with credentials; the server accepts the credentials and the session is authenticated; see also pages 22-23; Pkg #1 (with credentials) from Client; information inside XML Tag 'type' includes <auth-basic> and <auth-md5>)*.

- **Regarding claim 55**, SyncML, SyncML-DMS, Quick, Beatson, and Lahteenmaki disclose the method according to claim 54.

SyncML further discloses executing at the server authentication operations according to one of the plurality of authentication capabilities indicated in the authentication method list *(SyncML: page 21, section 3.5; the client sends Pkg #1 with the credentials; the server accepts the credentials and the session is authenticated; see also page 25; Fig. 6)*;

preparing a message at the server comprising the authentication method indicator and any authentication data relating to the specified authentication method *(SyncML: pages 21-23; see Pkg #2 from server)*; and

transmitting the message to the electronic communication apparatus *(SyncML: page 25, Fig. 6; Pkg #2: server initialization package to client)*.

- **Regarding claim 56**, SyncML, SyncML-DMS, Quick, Beatson, and Lahteenmaki disclose the method according to claim 55.

SyncML further discloses receiving the message at the electronic communication apparatus *(SyncML: page 25; Fig. 6; server initialization package to client)*;

executing, at the electronic communication apparatus, authentication operations according to the authentication method indicated by the authentication method indicator to generate an expected result *(SyncML: page 21, section 3.5; the client sends Pkg #1 with the credentials; the server accepts the credentials and the session is authenticated; see also page 25; Fig. 6)*;

preparing a response to the server comprising the authentication method indicator, and any authentication data *(SyncML: page 26, section 4.1; initialization requirements for client; see also page 33; Fig. 7; client makes data update for its databases)*; and

transmitting the response to the server *(SyncML: page 26, section 4.1; initialization requirements for client; see also page 33; Fig. 7; client sends server Pkg #5, data update status package)*.

- **Regarding claim 57**, SyncML, SyncML-DMS, Quick, Beatson, and Lahteenmaki disclose the method according to claim 46.

Quick further discloses the authentication method is Subscriber Identify Module/Universal Subscriber Identify Module (SIM/USIM) authentication, the method further comprising: using CKs/IKs (cipher keys/integrity keys) generated by the electronic communication apparatus and the server, respectively, to provide integrity protection *(Quick: pars. 0024 and 0026-0027; cipherkey 290 and integrity key 310)*, wherein the CKs/IKs are used for generating MAC values *(Quick: pars. 0026; the IK 310 can be used to generate a message authentication code MAC)*; and using a hashing function for computing a Hashed Method Authentication Code (HMAC) on the message *(Quick: par. 0038; HMAC-SHA-1 scheme; HMAC is implemented in the subscriber identification token)*.

10. **Claim 53 is rejected under 35 U.S.C. 103(a)** as being unpatentable over SyncML, SyncML-DMS, Quick, Beatson, and Lahteenmaki, as applied to claim 46 above, and further in view of Tran et al., (hereinafter "Tran"), U.S. Patent Application No. 2003/0033524, filed on August 13, 2001.

- **Regarding claim 53**, SyncML, SyncML-DMS, Quick, Beatson, and Lahteenmaki disclose the method according to claim 46.

SyncML, SyncML-DMS, Quick, Beatson, and Lahteenmaki do not explicitly disclose the authentication method is SecureId or SafeWord authentication.

However, in an analogous art, Tran discloses a wireless portal system, wherein the authentication method is SecureId or SafeWord authentication *(Tran: par. 0052; the authentication modules may also include LDAP authentication, secure ID, radius authentication, etc.)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Tran with the method of SyncML, SyncML-DMS, Quick, Beatson, and Lahteenmaki wherein the authentication method is SecureId or SafeWord authentication to provide access to any type of service from any type of device from anywhere and to provide content suitable for these devices without incurring substantial cost overhead *(Tran: par. 0008)*.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the

advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437